

# On Quantum Algorithms for Noncommutative Hidden Subgroups

Mark Ettinger<sup>1,\*</sup>

Peter Høyer<sup>2,1,†</sup>

<sup>1</sup> *Los Alamos National Laboratory*

<sup>2</sup> *Odense University*

Report No. LA-UR-98-2010 (May 6, 1998)

## Abstract

Quantum algorithms for factoring and discrete logarithm have previously been generalized to finding hidden subgroups of finite Abelian groups. This paper explores the possibility of extending this general viewpoint to finding hidden subgroups of noncommutative groups. We present a quantum algorithm for the special case of dihedral groups which determines the hidden subgroup in a linear number of calls to the input function. We also explore the difficulties of developing an algorithm to process the data to explicitly calculate a generating set for the subgroup. A general framework for the noncommutative hidden subgroup problem is discussed and we indicate future research directions.

## 1 Introduction

All known quantum algorithms which run super-polynomially faster than the most efficient probabilistic classical algorithm solve special cases of what is called the Abelian Hidden Subgroup Problem. This general formulation includes Shor's algorithms for factoring and finding discrete logarithms [16]. A very natural question to ask is if quantum computers can efficiently solve the Hidden Subgroup Problem in *noncommutative* groups. This question has been raised regularly [1, 11, 12, 13], and seems important for at least three reasons.

The first reason is that determining if two graphs are isomorphic reduces to finding hidden subgroups of symmetric groups. The second reason is that

---

\* Email: [ettinger@lanl.gov](mailto:ettinger@lanl.gov).

† Email: [u2pi@imada.ou.dk](mailto:u2pi@imada.ou.dk).

the noncommutative hidden subgroup problem arguably represents a most natural line of research in the area of quantum algorithmics. The third reason is that an efficient quantum algorithm for a hidden subgroup problem could potentially be used to show an exponential gap between quantum and classical two-party probabilistic communication complexity models [7, 6].

The heart of the idea behind the quantum solution to the Abelian hidden subgroup problem is Fourier analysis on Abelian groups. The difficulties of Fourier analysis on noncommutative groups makes the noncommutative version of the problem very challenging.

In this paper, we present the first known quantum algorithm for a noncommutative subgroup problem. We focus on dihedral groups because they are well-structured noncommutative groups, and because they contain an exponentially large number of different subgroups of small order, making classical guessing infeasible. Our main result is that there exists a quantum algorithm that solves the dihedral subgroup problem using only a linear number of evaluations of the function which is given as input. This is the first time such a result has been obtained for a noncommutative group. However, we hasten to add that our algorithm does *not* run in polynomial time, even though it only uses few evaluations of the given function. The reason for this is as follows: The algorithm applies a certain quantum subroutine a linear number of times, each time producing some output data. The collection of all the output data determines the hidden subgroup with high probability. We know how to find the subgroup from the data in exponential time, but we do not know if this task can be done efficiently.

Three important questions are left open. The first question is if there exists a polynomial-time algorithm (classical or quantum) to postprocess the output data from our quantum subroutine. The second is whether our algorithm can be used to show an exponential gap between quantum and classical probabilistic communication complexity models, as mentioned above. Currently, the state-of-the-art is an exponential separation between error-free models, and a quadratic separation between probabilistic models [6]. The third open question is for what other noncommutative groups similar results can be obtained.

## 2 Algorithm for dihedral groups

The *Hidden Subgroup Problem* is defined as follows:

**Given:** A function  $\gamma : G \rightarrow R$ , where  $G$  is a finite group and  $R$  an arbitrary finite range.

**Promise:** There exists a subgroup  $H \leq G$  such that  $\gamma$  is *constant* and *distinct* on the left cosets of  $H$ .

**Problem:** Find a generating set for  $H$ .

We say of such a function  $\gamma$  that it *fulfills the subgroup promise* with respect to  $H$ . We also say of  $\gamma$  that it *has hidden subgroup  $H$* . Note that we are not given the order of  $H$ . Without loss of generality we assume  $\gamma$  is constant and distinct on *left* cosets because we may formally rename group elements and convert multiplication on the right to multiplication on the left.

If  $G$  is Abelian, then we refer to this problem as the Abelian Subgroup Problem. Similarly, if the given group is dihedral, then we refer to it as the Dihedral Subgroup Problem. Classically, if  $\gamma$  is given as a black box, then the Abelian subgroup problem is infeasible: If  $G = \mathbb{Z}_2^n$ , then just to determine if  $H$  is non-trivial or not takes time exponential in  $n$  [17]. Here,  $\mathbb{Z}_2$  denotes the cyclic group of order 2. In contrast, the Abelian subgroup problem can be solved efficiently on a quantum computer [3, 5, 8, 13, 16, 17].

**Theorem 1** *Let  $\gamma : G \rightarrow R$  be a function that fulfills the Abelian subgroup promise with respect to  $H$ . There exists a quantum algorithm that outputs a subset  $X \subseteq G$  such that  $X$  is a generating set for  $H$  with probability at least  $1 - 1/|G|$ , where  $|G|$  denotes the order of  $G$ . The algorithm uses  $O(\log |G|)$  evaluations of  $\gamma$ , and runs in time polynomial in  $\log |G|$  and in the time required to compute  $\gamma$ .*

We review the quantum solution to the Abelian subgroup problem in terms of group representation theory in Section 4 below. For other reviews, see for example [4, 12].

The dihedral group of order  $2N$  is the symmetry group of an  $N$ -sided polygon. It is a semidirect product of the two cyclic groups  $\mathbb{Z}_N$  and  $\mathbb{Z}_2$  of order  $N$  and 2, respectively. It is isomorphic to the group

$$D_N = \mathbb{Z}_N \rtimes_{\phi} \mathbb{Z}_2 \tag{1}$$

with the multiplication defined by

$$(a_1, b_1)(a_2, b_2) = (a_1 + \phi(b_1)(a_2), b_1 + b_2),$$

where the homomorphism  $\phi : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_N)$  is defined by  $1 \mapsto \phi(1)(a) = -a$ .

**Theorem 2 (Main theorem)** *Let  $\gamma : D_N \rightarrow R$  be a function that fulfills the dihedral subgroup promise with respect to  $H$ . There exists a quantum algorithm that given  $\gamma$ , uses  $\Theta(\log N)$  evaluations of  $\gamma$  and outputs a subset  $X \subseteq D_N$  such that  $X$  is a generating set for  $H$  with probability at least  $1 - \frac{2}{N}$ .*

Theorem 2 constitutes our main result that the dihedral subgroup problem can be solved with few applications of the given function  $\gamma$ . The essential step in the proof is that it is possible to find subgroups of order 2. The dihedral group  $D_N$  contains  $N + 1$  different subgroups of order 2 if  $N$  is even, and  $N$  different subgroups of order 2 if  $N$  is odd.

So, even if we are promised that the hidden subgroup is of that order, a straight-forward approach to find its generator would take time exponential in  $\log(N)$ . Theorem 3 entails that we can find the generator with an expected number of evaluations of  $\gamma$  only linear in  $\log N$ .

**Theorem 3** *Let  $\gamma : D_N \rightarrow R$  be a function that fulfills the dihedral subgroup promise with respect to  $H$ , where  $H$  is either the trivial subgroup, or  $H = \{(0,0), (k_0, 1)\}$  for some  $0 \leq k_0 < N$ . There exists a quantum algorithm that given  $\gamma$ , uses at most  $89 \log(N) + 7$  evaluations of  $\gamma$  and outputs either “trivial” or the value  $k_0$ . If  $H$  is trivial then the output is always “trivial”, and if  $H$  is non-trivial then the algorithm outputs  $k_0$  with probability at least  $1 - \frac{1}{2N}$ .*

We first give the reduction of the general problem given in Theorem 2 to the special case in Theorem 3.

**Proof of Theorem 2** Let  $\gamma_1$  denote the restriction of  $\gamma$  to the cyclic subgroup  $\mathbb{Z}_N \times \{0\} \leq D_N$  of order  $N$ . Then  $\gamma_1 : \mathbb{Z}_N \times \{0\} \rightarrow R$  fulfills the Abelian subgroup promise with respect to  $H_1 = H \cap (\mathbb{Z}_N \times \{0\})$ . By Theorem 1, we can, by using  $O(\log N)$  evaluations of  $\gamma_1$ , find a subset  $X_1 \subseteq H_1$  so that  $X_1$  generates  $H_1$  with probability at least  $1 - 1/N$ .

The subgroup  $\langle X_1 \rangle \leq D_N$  is normal in  $D_N$ , and the factor group  $D_N / \langle X_1 \rangle$  is isomorphic to  $D_M$  where  $M = \min\{1 \leq j \leq N \mid (j, 0) \in \langle X_1 \rangle\}$ . Since  $\gamma$  is constant on the cosets of  $\langle X_1 \rangle$ , we can consider  $\gamma$  a function  $\gamma_2$  on  $D_M$ . Then  $\gamma_2 : D_M \rightarrow R$  fulfills the dihedral subgroup promise with respect to some subgroup  $H_2 \leq D_M$ .

Suppose  $\langle X_1 \rangle = H_1$ . Then either  $H_2 = \{(0,0)\}$  is the trivial subgroup, or  $H_2 = \{(0,0), (k_0, 1)\}$  for some  $0 \leq k_0 < M$ . Further, if  $H_2$  is trivial then  $H = \langle X_1 \rangle$ , and if  $H_2 = \{(0,0), (k_0, 1)\}$  then  $H = \langle X_1, (k_0, 1) \rangle$ .

We now apply the algorithm in Theorem 3 with  $\gamma_2 : D_M \rightarrow R$ , producing either “trivial” or  $k_0$ . We repeat this  $t = \lceil \log(2N) / \log(2M) \rceil$  times in total, ensuring we will find  $k_0$  with probability at least  $1 - 1/(2M)^t \geq 1 - 1/2N$ , provided  $k_0$  exists. If we obtain  $k_0$ , then let  $X = X_1 \cup \{(k_0, 1)\}$ , and otherwise let  $X = X_1$ .

If  $X_1$  generates  $H_1$ , then with probability at least  $1 - 1/2N$  we have  $H = \langle X \rangle$ . Since  $X_1$  generates  $H_1$  with probability at least  $1 - 1/N$ , the overall success probability is at least  $(1 - 1/N)(1 - 1/2N) > 1 - 2/N$ . The

total number of evaluations of  $\gamma$  is at most  $O(\log N) + t(89 \log M + 7)$ , as each evaluation of  $\gamma_1$  and  $\gamma_2$  requires one evaluation of  $\gamma$ .  $\square$

We assume that the reader is familiar with the basic notions of quantum computation [2]. The quantum algorithm we shall use to prove Theorem 3 is

$$\mathbf{V}_\gamma = (\mathbf{F}_N \otimes \mathbf{W} \otimes \mathbf{I}) \circ \mathbf{U}_\gamma \circ (\mathbf{F}_N^{-1} \otimes \mathbf{W} \otimes \mathbf{I}). \quad (2)$$

Here,  $\mathbf{U}_\gamma$  is any unitary operator that satisfies that

$$\mathbf{U}_\gamma |a\rangle|b\rangle|0\rangle = |a\rangle|b\rangle|\gamma(a, b)\rangle \quad (3)$$

for all  $0 \leq a < N$  and  $0 \leq b \leq 1$ . The operator  $\mathbf{F}_N$  is the quantum Fourier transform for  $\mathbb{Z}_N$  defined by

$$\mathbf{F}_N |i\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{ij} |j\rangle, \quad (4)$$

where  $\omega_N = e^{2\pi\sqrt{-1}/N}$  is the  $N$ th principal root of unity. When  $N = 2$ , then the Fourier transform  $\mathbf{F}_2$  is equal to the Walsh–Hadamard transform  $\mathbf{W}$  which maps a qubit in state  $|b\rangle$  to the superposition  $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$ .

Suppose for a moment that we were not given a function defined on the dihedral group  $D_N = \mathbb{Z}_N \rtimes_\phi \mathbb{Z}_2$ , but instead a function defined on the Abelian group  $\mathbb{Z}_N \times \mathbb{Z}_2$ . Or equivalently, suppose for the moment that  $\phi : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_N)$  is the trivial homomorphism. Then by Theorem 1, we can find any hidden subgroup with probability exponentially close to 1 by applying the experiment

$$(a, b) = \mathcal{M}_{1,2} \circ \mathbf{V}_\gamma |0\rangle|0\rangle|0\rangle \quad (5)$$

a number of  $O(\log N)$  times. Here,  $\mathcal{M}_{1,2}$  denotes a measurement of the first two registers with outcome  $(a, b)$ . A natural question to ask is, how much information, if any, would we gain by performing the experiment given in Equation 5 when  $\gamma$  is defined on  $D_N$  and not on  $\mathbb{Z}_N \times \mathbb{Z}_2$ . The next lemma shows that we indeed learn something.

**Lemma 4** *Let  $\gamma : D_N \rightarrow R$  fulfill the subgroup promise with respect to  $H = \{(0, 0), (k_0, 1)\}$ . Then, if we apply quantum algorithm  $\mathbf{V}_\gamma$  on the initial state  $|0\rangle|0\rangle|0\rangle$ , the probability that the outcome of a measurement of the first two registers is  $(a, 0)$ , is*

$$\frac{1}{2N} (1 + \cos(2\pi k_0 a / N)) = \frac{1}{N} \cos^2(\pi k_0 a / N). \quad (6)$$

*Furthermore, the probability that the outcome is  $(a, 1)$ , is  $\frac{1}{N} \sin^2(\pi k_0 a / N)$ .*

Let  $\mathbf{Z}$  denote the discrete random variable defined by the probability mass function

$$\text{Prob}[\mathbf{Z} = z] = \alpha \cos^2(\pi k_0 z / N) \quad (z \in \mathbb{Z}_N),$$

where  $\alpha = 1/N$  if  $k_0 = 0$  or  $2k_0 = N$ , and  $\alpha = 2/N$  otherwise. Lemma 4 provides us with a quantum algorithm for sampling from  $\mathbf{Z}$ . Intuitively, since  $\mathbf{Z}$  is non-uniformly distributed on  $\mathbb{Z}_N$  depending on  $k_0$ , the more samples we draw from  $\mathbf{Z}$ , the more knowledge we gather about  $k_0$ . The crucial question therefore becomes, how many samples from  $\mathbf{Z}$  do we need to be able to identify  $k_0$  correctly with high probability. Theorem 5 below states that we only need a logarithmic number of samples. We postpone its proof till the next section.

**Theorem 5** *Let  $m \geq \lceil 64 \ln N \rceil$ , and let  $z_1, \dots, z_m$  be independent samples from  $\mathbf{Z}$ . Let  $\tilde{k} \in \{1, \dots, \lfloor N/2 \rfloor\}$  be such that the sum  $\sum_{i=1}^m \cos(2\pi \tilde{k} z_i / N)$  is maximal. Then  $\tilde{k} = \min\{k_0, N - k_0\}$  with probability at least  $1 - \frac{1}{2N}$ .*

**Proof of Theorem 3** The algorithm starts by disposing the possibility that  $k_0 = 0$  by computing  $\gamma(0, 0)$  and  $\gamma(0, 1)$ . If the two values are equal, then the algorithm outputs the value 0 and stops. If  $N$  is even, then the algorithm proceeds by disposing the possibility that  $k_0 = N/2$ , too.

Now, the algorithm applies the quantum experiment given in Equation 5 a number of  $m' = 2\lceil 64 \ln N \rceil$  times. Let  $m$  denote the number of times it measures a 0 in the second register. Let  $\{a_1, \dots, a_m\}$  denote the outcomes in the first register, conditioned to that the measurement of the second register yields a zero.<sup>1</sup>

Suppose  $m \geq m'/2$ . The algorithm continues with classical post-processing: It finds  $1 \leq \tilde{k} \leq \lfloor N/2 \rfloor$  such that the sum  $\sum_{i=1}^m \cos(2\pi \tilde{k} a_i / N)$  is maximized. It then computes  $\gamma(\tilde{k}, 1)$  and compares it with the previous calculated value  $\gamma(0, 0)$ . If they are equal, it outputs  $\tilde{k}$  and stops. Otherwise, it performs the same test for  $\gamma(N - \tilde{k}, 1)$ . If that one also fails, it outputs “trivial”.

If  $m < m'/2$ , then the algorithm performs the same classical post-processing, except that it uses the  $m' - m$  measurements for which the output in the second register is 1, and except that it now seeks to maximize the sum  $\sum_{i=1}^m \sin(2\pi \tilde{k} a_i / N)$ .

If  $H$  is trivial, then the algorithm returns “trivial” with certainty. If  $H = \{(0, 0), (k_0, 1)\}$ , then it outputs  $k_0$  with probability at least  $1 - 1/2N$  by Theorem 5. The total number of evaluations of  $\gamma$  is upper bounded by  $m' + 5 < 89 \log N + 7$ .  $\square$

---

<sup>1</sup> Alternatively, we could apply amplitude amplification [5] to ensure that we will always measure 0 in the second register, instead of as here, only with probability  $1/2$ .

### 3 Proof of Theorem 5

The proof of Theorem 5 requires two lemmas, the first of them being a result by Hoeffding [10] on the sum of bounded random variables. Hoeffding's lemma says that the probability that the sum of  $m$  independent samples are off from its expected value by a constant fraction in  $m$  drops exponentially in  $m$ .

**Lemma 6 (Hoeffding)** *Let  $\mathbf{X}_1, \dots, \mathbf{X}_m$  be independent identically distributed random variables with  $\ell \leq \mathbf{X}_1 \leq u$ . Then, for all  $\alpha > 0$ ,*

$$\text{Prob}[\mathbf{S} - \mathbf{E}[\mathbf{S}] \geq \alpha m] \leq e^{-2\alpha^2 m / (u - \ell)^2}$$

where  $\mathbf{S} = \sum_{i=1}^m \mathbf{X}_i$ .

Let  $0 < k < N$ , and suppose we want to test if  $k \stackrel{?}{=} k_0$  or  $k \stackrel{?}{=} N - k_0$ , where  $k_0$  is given as in Lemma 4. Clearly, we can answer that question just by testing if  $\gamma(0, 0) \stackrel{?}{=} \gamma(k, 1)$  or  $\gamma(0, 0) \stackrel{?}{=} \gamma(N - k, 1)$ . Lemma 7 provides us with another probabilistic method: First draw  $m$  samples  $\{z_i\}_{i=1}^m$  from  $\mathbf{Z}$ , and then compute the sum  $\sum_{i=1}^m \cos(2\pi k z_i / N)$ . Conclude that  $k \neq k_0$  and  $k \neq N - k_0$  if and only if that sum is at most  $m/4$ .

**Lemma 7** *Let  $0 < k < N$ . Let  $z_1, \dots, z_m$  be  $m$  independent samples from  $\mathbf{Z}$ . Then with probability at most  $e^{-m/32}$ , we have*

$$\sum_{i=1}^m \cos(2\pi k z_i / N) \leq m/4$$

if  $k = k_0$  or  $k = N - k_0$ , and

$$\sum_{i=1}^m \cos(2\pi k z_i / N) \geq m/4$$

otherwise.

**Proof** Let  $f$  denote the function of  $\mathbf{Z}$  defined by  $f(z) = \cos(2\pi k z / N)$ , and let  $\mathbf{X} = f(\mathbf{Z})$  denote the random variable defined by  $f$ . Then  $-1 \leq \mathbf{X} \leq 1$  and the expected value of  $\mathbf{X}$  is

$$\mathbf{E}[\mathbf{X}] = \begin{cases} 1 & \text{if } 2k = 2k_0 = N \\ \frac{1}{2} & \text{if either } k = k_0 \text{ or } k = N - k_0 \\ 0 & \text{otherwise.} \end{cases}$$

If  $k \neq k_0$  and  $k \neq N - k_0$ , then apply Hoeffding's lemma on  $m$  independent random variables all having the same probability distribution as  $\mathbf{X}$ . If  $k = k_0$  or  $k = N - k_0$ , then apply Hoeffding's lemma on  $m$  independent random variables all having the same probability distribution as the random variable  $\mathbb{E}[\mathbf{X}] - \mathbf{X}$ .  $\square$

If we are only concerned about testing for a specific  $0 < k < N$  if  $k \stackrel{?}{=} k_0$  or  $k \stackrel{?}{=} N - k_0$ , then Lemma 7 is not beneficial since we could just test if  $\gamma(0, 0) \stackrel{?}{=} \gamma(k, 1)$  or  $\gamma(0, 0) \stackrel{?}{=} \gamma(N - k, 1)$ . But since we want to test all possible values of  $k$ , and not only a single one, then the method yielded by Lemma 7 becomes valuable, provided we can reuse the same  $m$  samples in all tests. We now prove Theorem 5 by showing that, given a set of  $m$  samples, then it is very likely that the sum  $\sum_{i=1}^m \cos(2\pi k z_i / N)$  is larger than  $m/4$  if and only if  $k = k_0$  or  $k = N - k_0$ .

**Proof of Theorem 5** This is a simple consequence of Lemma 7. Let  $k'_0 = \min\{k_0, N - k_0\}$ . The probability that  $\sum_{i=1}^m \cos(2\pi k'_0 z_i / N) \leq m/4$  is at most  $e^{-m/32} \leq \frac{1}{N^2}$ . Furthermore, for all integers  $0 < k \leq N/2$  not equal to  $k'_0$ , the probability that  $\sum_{i=1}^m \cos(2\pi k z_i / N) \geq m/4$  is also at most  $\frac{1}{N^2}$ . If  $\tilde{k} \neq k'_0$ , then one of these  $\lfloor N/2 \rfloor$  events must have happened, and the probability for that is upper bounded by  $\lfloor \frac{N}{2} \rfloor \frac{1}{N^2} \leq \frac{1}{2N}$ .  $\square$

## 4 Abelian Hidden Subgroups

Theorem 1 in Section 2 states that the Abelian subgroup problem can be solved efficiently on a quantum computer. The algorithm which accomplishes this is most easily understood using some basic representation theory for finite Abelian groups which we now briefly review. For more details see the excellent references [14, 15]. For any Abelian group  $G$  the group algebra  $\mathbb{C}[G]$  is the Hilbert space of all complex-valued functions on  $G$  equipped with the standard inner product. A *character* of  $G$  is a homomorphism from  $G$  to  $\mathbb{C}$ . The set of characters admits a natural group structure via pointwise multiplication and is a basis for the group algebra. The *Fourier transform* is the linear transformation from the point mass basis of the group algebra to the basis of characters. It is known that the quantum Fourier transform may be performed in time  $O(\log^2 |G|)$ . Finally, for any subgroup  $H \leq G$ , there exists a subgroup of the character group called the orthogonal subgroup  $H^\perp$  which consists of all characters  $\chi$  such that  $\chi(h) = 1$  for all  $h \in H$ .

We now sketch the quantum algorithm for solving the Abelian hidden subgroup problem. In the interest of clarity we omit all normalization factors in



our description. The state of the computer is initialized in the superposition

$$\sum_{g \in G} |g\rangle |\gamma(g)\rangle.$$

We then observe the second register with outcome, say,  $r \in R$ . This action serves to place the first register into a superposition of all elements that map to  $r$  under  $\gamma$ . Because  $\gamma$  is constant and distinct on cosets of  $H$  we may write the state of the computer as

$$\sum_{h \in H} |s + h\rangle |r\rangle$$

for some coset  $s + H$  chosen by the observation of the second register. Since we will not use the second register or its contents in the remainder of the algorithm, we express the state of the computer as a function of the contents of the first register only,  $\sum_{h \in H} |s + h\rangle$ . We then apply the quantum Fourier transform which results in the state

$$\sum_{h' \in H^\perp} \langle h' | s \rangle |h'\rangle,$$

which may be verified by direct calculation. Finally, we observe the first register. Notice that this results in a uniformly random sample from  $H^\perp$ .

It can easily be shown that by repeating this experiment of order  $\log |H^\perp|$  times, we find a generating set for  $H^\perp$ . The hidden subgroup  $H \leq G$  can then be calculated efficiently from  $H^\perp$  on a classical computer, essentially by linear algebra. In summary, the sole purpose of the quantum machine in the above algorithm is to sample uniformly from  $H^\perp$ .

## 5 A Generalized $H^\perp$

We now briefly discuss the main ideas of harmonic analysis on groups, stating as facts the main results that we require. For more detailed information see the excellent references [14, 15]. Let  $G$  be a (possibly noncommutative) finite group. A representation of  $G$  is a homomorphism  $\rho : G \rightarrow GL(V_\rho)$  where  $V_\rho$  is called the *representation space* of the representation. The dimension of  $V_\rho$ , denoted  $d_\rho$ , is called the dimension of the representation. The representation  $\rho$  is *irreducible* if the only invariant subspaces of  $V_\rho$  are 0 and  $V_\rho$  itself. Two representations  $\rho_1$  and  $\rho_2$  are *equivalent* if there exists an invertible linear map  $S : V_{\rho_1} \rightarrow V_{\rho_2}$  such that  $\rho_1(g) = S^{-1} \rho_2(g) S$  for all  $g \in G$ .

Let  $\Gamma = \{\rho_1, \rho_2, \dots, \rho_r\}$  be a complete set of inequivalent, irreducible representations of  $G$ . Then the identity  $\sum_{i=1}^r d_{\rho_i}^2 = |G|$  holds. Furthermore, we

may assume that the representations are unitary, i.e., that  $\rho(g)$  is a unitary matrix for all  $g \in G$  and all  $\rho \in \Gamma$ . The functions defined by  $\rho_{ij} = \rho(g)_{ij}$  for  $1 \leq i, j \leq d_\rho$  are called *matrix coefficients*, and by the previous identity it follows that there are  $|G|$  matrix coefficients. It is a fundamental fact that the set of all *normalized* matrix coefficients obtained from any fixed  $\Gamma$  is an orthonormal basis of the group algebra  $\mathbb{C}[G]$ . The *Fourier transform* (with respect to a chosen  $\Gamma$ ) is a change of basis transformation of the group algebra from the basis of point masses to the basis of matrix coefficients.

If  $G$  is commutative, then these definitions reduce to those discussed in the previous section, since in that case, all representations are 1-dimensional and each matrix coefficient is just a character. If  $G$  is noncommutative, then there exists at least 1 irreducible representation of  $G$  with higher dimension, and in this case the Fourier transform depends on the choice of bases for the irreducible representations. It seems as though this is what complicates the extension of the quantum algorithm for commutative groups to the noncommutative scenario.

It turns out that for our present application it is most useful to use an equivalent notion of the Fourier transform. One may also think of the matrix coefficients as collected together in matrices. In this view the Fourier transform is a matrix-valued function on  $\Gamma$ . For each  $f \in \mathbb{C}[G]$ , we define the value of the Fourier transform at an irreducible representation  $\rho \in \Gamma$  to be

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g) \rho(g).$$

If we take individual entries of these matrices, then we recover the coefficients in the basis of matrix coefficients. There is a Fourier inversion formula and therefore  $f$  is determined by the matrices  $\{\hat{f}(\rho)\}_{\rho \in \Gamma}$ .

We may now describe the noncommutative version of  $H^\perp$ . Let  $V_\rho^H$  be the elements of  $V_\rho$  that are *pointwise* fixed by  $H$ ,

$$V_\rho^H = \{v \in V_\rho \mid \rho(h)v = v, h \in H\}.$$

Let  $P_\rho^H$  be the projection operator onto  $V_\rho^H$ . Then define

$$H^\perp = \{P_\rho^H\}_{\rho \in \Gamma}.$$

The significance of this definition follows from the following elementary result.

**Theorem 8** *Let  $I_H$  be the indicator function on the subgroup  $H \leq G$ . Then, for all  $\rho \in \Gamma$ , we have that  $\hat{I}_H(\rho) = P_\rho^H$ .*

**Corollary 9** *Let  $sH$  be any coset of  $H \leq G$ . Then the previous theorem immediately yields  $\hat{I}_{sH}(\rho) = \rho(s)P_\rho^H$ .*

Let us briefly summarize the role of this result in the quantum algorithm. If we straight-forwardly apply the quantum algorithm described in the previous section to the case where  $G$  is noncommutative, then we must determine the resulting probability amplitudes and the information gained by sampling according to these amplitudes.

Recall that the state of the quantum system after the first observation is a superposition of states corresponding to the members of one coset. Thus the state may be described by the indicator function of a coset  $I_{sH}$ . The final observation results in observing the name of a matrix coefficient  $|\rho, i, j\rangle$ . The probability of observing  $|\rho, i, j\rangle$  is given by  $|c_{\rho, i, j}|^2$  where  $c_{\rho, i, j}$  is the coefficient of  $\rho_{ij}$  in the expansion of  $I_{sH}$  in the basis of matrix coefficients. The corollary above allows us, in theory, to compute these probability amplitudes.

The algorithm described in the first part of this paper may be derived from these general methods. For a general noncommutative group it seems that these methods are necessary for an analysis of the resulting probability amplitudes.

## 6 Acknowledgements

We would like to thank Dan Rockmore, David Maslen and Hans J. Munkholm from whom we learned noncommutative Fourier analysis, and Richard Hughes, Robert Beals and Joan Boyar for helpful conversations on this problem.

## References

- [1] BEALS, Robert, “Quantum computation of Fourier transforms over symmetric groups”, *Proceedings of the 29th Annual ACM Symposium on Theory of Computing — STOC*, 1997, pp. 48–53.
- [2] BERTHIAUME, André, “Quantum computation”, in *Complexity Theory Retrospective II*, L.A. Hemaspaandra and A.L. Selman (editors), Springer-Verlag, 1997.
- [3] BONEH, Dan and Richard J. LIPTON, “Quantum cryptanalysis of hidden linear functions (Extended abstract)”, *Proceedings of Advances in Cryptology — CRYPTO*, 1995, Lecture Notes of Computer Science, Vol. 963, Springer-Verlag, pp. 424–437.

- [4] BRASSARD, Gilles and Peter HØYER, “On the power of exact quantum polynomial time”, unpublished, 1996. Available on Los Alamos e-Print archive (<http://xxx.lanl.gov>) as quant-ph/9612017.
- [5] BRASSARD, Gilles and Peter HØYER, “An exact quantum polynomial-time algorithm for Simon’s problem”, *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems — ISTCS*, 1997, IEEE Computer Society Press, pp. 12–23.
- [6] BUHRMAN, Harry, Richard CLEVE and Avi WIGDERSON, “Quantum vs. classical communication and computation”, *Proceedings of the 30th Annual ACM Symposium on Theory of Computing — STOC*, 1998. To appear.
- [7] CLEVE, Richard and Harry BUHRMAN, “Substituting quantum entanglement for communication”, *Physical Review A*, Vol. 56, 1997, pp. 1201–1204.
- [8] GRIGORIEV, Dima, “Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines”, *Theoretical Computer Science*, Vol. 180, 1997, pp. 217–228.
- [9] *Groups and Computation II*, Proceedings of the 1996 DIMACS Workshop in Groups and Computation, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, L. Finkelstein and W. Kantor (editors), Vol. 28, American Mathematical Society, 1997.
- [10] Hoeffding, Wassily, “Probability inequalities for sums of bounded random variables”, *Journal of the American Statistical Association*, Vol. 58, 1963, pp. 13–30.
- [11] HØYER, Peter, “Efficient quantum transforms”, unpublished, 1997. Available on Los Alamos e-Print archive (<http://xxx.lanl.gov>) as quant-ph/9702028.
- [12] JOZSA, Richard, “Quantum algorithms and the Fourier transform”, *Proceedings of the Royal Society, London*, Vol. A454, 1998, pp. 323–337.
- [13] KITAEV, Alexey Yu., “Quantum measurements and the Abelian stabilizer problem”, unpublished, 1995. Available on Los Alamos e-Print archive (<http://xxx.lanl.gov>) as quant-ph/9511026.
- [14] MASLEN, David K. and Daniel N. ROCKMORE, “Generalized FFTs — A survey of some recent results”, pp. 183–238 in [9].

- [15] ROCKMORE, Daniel N., “Some applications of generalized FFTs”, pp. 329–370 in [9].
- [16] SHOR, Peter W., “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM Journal on Computing*, Vol. 26, 1997, pp. 1484–1509.
- [17] SIMON, Daniel R., “On the power of quantum computation”, *SIAM Journal on Computing*, Vol. 26, 1997, pp. 1474–1483.